Sujet n°1

La direction interministérielle des systèmes d'information et de communication (DISIC) a été créée par décret du 21 février 2011. Elle est chargée notamment d'organiser toutes les opérations de mutualisation des systèmes d'information entre les différentes administrations de l'Etat.

Dans ce contexte, vous êtes chargé par la DSIC d'étudier la mutualisation du service d'accès internet entre le ministère de l'intérieur et un autre ministère nommé ici Ministère B. Les évolutions devront a minima respecter la politique de sécurité et le niveau de qualité de service de chaque ministère. Le service d'accès internet regroupe dans le cadre de cette étude la navigation web et la messagerie vers internet. Votre étude portera également sur la mise en œuvre d'un plan de continuité des services internet et sur la refacturation de ces derniers au niveau des clients (directions utilisatrices).

Après avoir comparé les solutions mises en œuvre au sein de chaque ministère, vous préconiserez la solution de mutualisation qui vous paraît la plus efficiente en la justifiant et en l'argumentant. Vous préciserez les critères de performances pour une mise en œuvre opérationnelle prenant en compte les différents coûts induits.

Liste des documents

Document n°1 :	Page web du site du premier ministre intitulée Création de la DISIC pour mieux mutualiser les systèmes d'information et de communication de l'État - 20/04/2011	Page 1
Document n°2 :	Description du service internet du MIOMCTI	Pages 2 à 8
Document n°3 :	Description du service internet du ministère B	Pages 9 à 15
Document n°4 :	Le serveur mandataire , http://irp.nain-t.net « L'internet rapide et permanent »	Page 16
Document n°5 :	Présentation DSIC anti-spam et article sur le Greylisting du site radical-spam	Page 17
Document n°6 :	Communiqué de presse de l'association signal spam sur la convention de partenariat signée avec l'OCLCTIC – 4 mai 2011	Pages 18 à 19
Document n°7 :	Extrait d'une FAQ du site http://www.squid-cache.org intitulé « Communication between browsers and Squid »	Pages 20 à 22
Document n°8 :	ISO 22301 : la future norme de Continuité d'activité, source http://www.duquesnegroup.com 28/01/2011	Pages 23 à 25
Document n°9 :	«Refacturation en interne des prestations informatiques : mode d'emploi » de F. Bordage en 2007 sur le site web indexel.net	Page 26
Document n°10 :	Extrait du projet d'offre de service DSIC en 2011	Pages 27 à 29

Création de la Disic pour mieux mutualiser les systèmes d'information et de communication de l'État

Création de la Disic pour mieux mutualiser les systèmes d'information et de communication de l'État

Placée sous l'autorité du Premier ministre, la Direction interministérielle des systèmes d'information et de communication (Disic)(1) est rattachée au Secrétaire général du Gouvernement (SGG). Véritable DSI interministérielle, elle aura pour missions d'**organiser la mutualisation interministérielle des systèmes d'information** et de **définir une stratégie globale pour développer les systèmes d'information et de communication des administrations de l'Etat**.

Une plus grande cohérence grâce à la mutualisation

La Disic aura un rôle stratégique notamment en se penchant sur toutes les actions à mettre en oeuvre pour pouvoir **mutualiser des ressources entre plusieurs administrations de l'Etat, ou entre des administrations de l'Etat et d'autres autorités administratives**. Pour cela, elle pilotera elle-même certains projets de mutualisation ou, a minima, sera associée au pilotage.

La Disic sera enfin en mesure de conseiller et d'alerter le Premier ministre ou les ministères concernés sur les "enjeux et risques relatifs à des projets d'importance majeure".

L'objectif est de permettre aux administrations de l'Etat d'anticiper les évolutions des technologies et du marché, de même que les besoins, et de gagner en efficacité. Une visibilité qui permettra de fixer les orientations en matière d'externalisation, de sous-traitance et d'achats de matériels, logiciels et prestations de services. Avec au bout de la chaîne, une simplification des relations entre usagers et administrations.

1. Elle se substitue au Comité de pilotage national des systèmes d'information (CPNSI) mis en place en juin 2009 (source : Direction générale de la modernisation de l'État). ↵

Politiques publiques

Fonction publique
http://www.gouvernement.fr/taxonomy/term/36
Société de l'information
http://www.gouvernement.fr/taxonomy/term/6
Etat et collectivités
http://www.gouvernement.fr/node/91

URL source: http://www.gouvernement.fr/gouvernement/creation-de-la-disic-pour-mieux-mutualiser-les-systemes-d-information-et-de-communicati
Créé 2011-04-20 06:22

Liens:
[1] http://www.gouvernement.fr/gouvernement/creation-de-la-disic-pour-mieux-mutualiser-les-systemes-d-information-et-de-communicati#fn:1
[2] http://www.gouvernement.fr/gouvernement/creation-de-la-disic-pour-mieux-mutualiser-les-systemes-d-information-et-de-communicati#fnref:1
[3] http://www.gouvernement.fr/node/80534
[4] http://www.legifrance.gouv.fr/affichTexte.do

Description du service internet du Ministère de l'Intérieur,

de l'Outre-Mer, des Collectivités Territoriales et de l'Immigration

1. Présentation générale

La passerelle d'accès à internet assure l'interface entre l'intranet du Ministère et internet. Elle isole le réseau du Ministère et masque son plan d'adressage interne. Elle filtre le trafic web et messagerie et protège le Ministère contre les tentatives d'intrusion ou d'entrée de virus informatique. Elle autorise la consultation des pages Web en fonction des profils utilisateurs et du classement des sites.

Au niveau messagerie, elle donne la possibilité aux utilisateurs possédant une boîte aux lettres sur la messagerie interne du Ministère d'échanger des messages électroniques avec le monde internet sous certaines conditions.

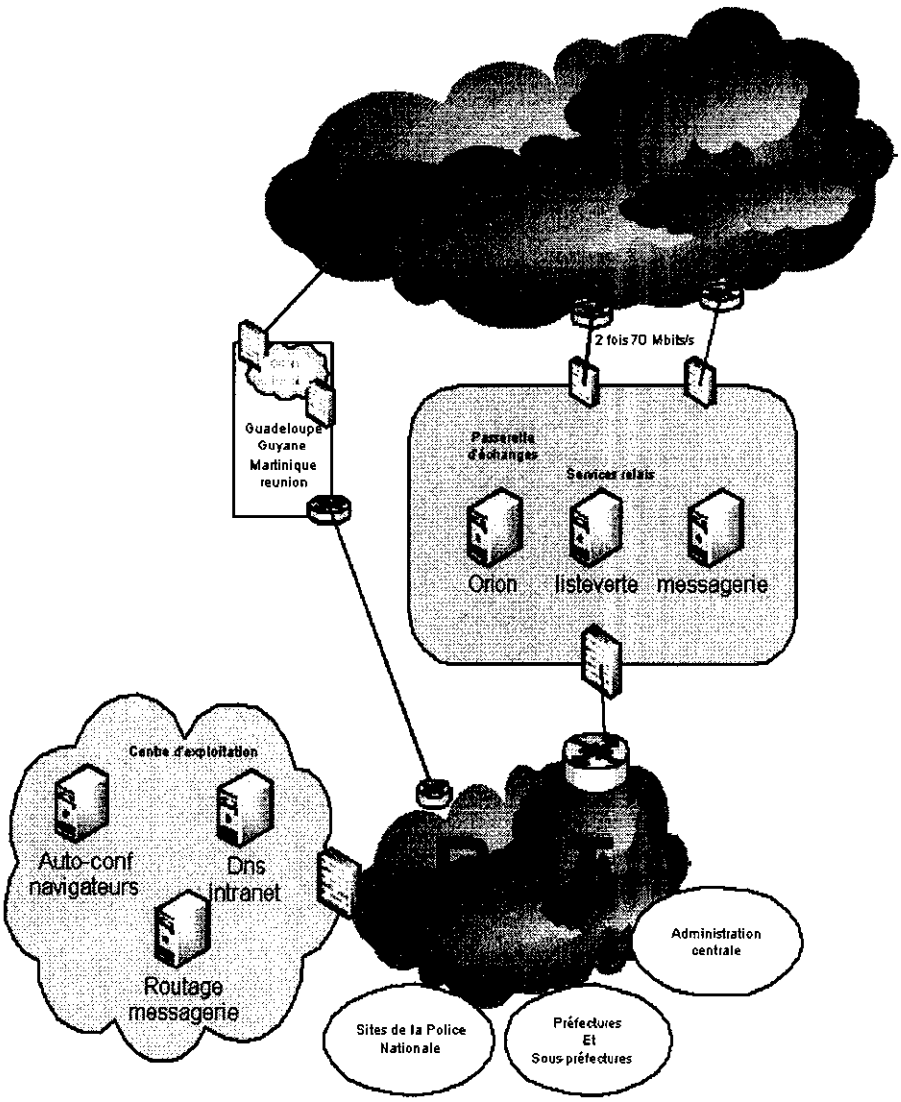
1.1. Schéma de principe

Le schéma ci-dessous représente l'architecture du service internet du Ministère de l'intérieur.
La passerelle d'échanges du ministère abrite des chaînes de relais web et messagerie internet pour le Ministère.

Le service d'accès web se compose de deux chaînes distinctes pour les clients du RGT:

- **la chaîne Orion:** Consultation des sites Internet

- **La chaîne Liste verte:** L'accès aux sites gouvernementaux et métiers sur Internet et d'autres réseaux privés



1.2. Ressources impactées par le service internet

Liste des différents acteurs du Ministère de l'Intérieur impactés par le service internet:

- Le centre d'appel qui gère les appels clients et ouvrent les incidents
- Les responsables de la sécurité des systèmes d'information
- L'équipe d'administration et d'exploitation (2 ETP de charge)
- L'équipe de conception, d'intégration et de support technique
- l'équipe de supervision H24

1.3. Fonctionnement

Les navigateurs des postes clients sont paramétrés pour télécharger un script d'auto-configuration (proxy pac, config.mi) qui permet d'orienter les requêtes web vers les domaines internes et externes sur les relais ou serveurs adéquats.

Principe d'aiguillage:

- les urls en .mi sont envoyées en direct sur l'intranet,
- les urls en .gouv.fr (par exemple) sont envoyées vers le service liste verte,
- et le reste des urls est dirigée par défaut vers le service Orion.

1.4. Eléments quantitatifs

- Service de messagerie internet
  - 145 mille comptes de messagerie internes
  - 200 000 msg/jour entrant depuis internet vers le MI
  - 140 000 msg/jour sortant vers internet depuis le MI
  - 50 à 60 Go/jour de données transitant par les passerelles Internet
  - environ 2 à 3% de spams ou pourriels (5 000 messages)
  - disponibilité de 99,99%

- Service Web
  - 80 mille clients avec profil ORION. 130 mille clients potentiels sur la Liste Verte.
  - 65 millions de connexions / jour - 400 Giga-octets
  - temps de réponse moyen du service orion : 930 ms (8h-18h00)
  - temps de réponse moyen du service listeVerte : < 100 ms (8h-18h00)
  - disponibilité de 99,97%

1.5. Accès réseau internet

La bande passante internet est de 140 Mbits/s divisés en deux liens de 70 Mbits. Le coût mensuel de cet accès s'élève à 9k€.

Le premier lien est réservé en mode nominal aux flux web métiers et à la messagerie.

Le second lien est réservé en mode nominal aux flux internet web non privilégiés.

En cas de panne d'un lien, l'autre récupère automatiquement l'ensemble des flux. Il est nécessaire ensuite de brider la bande passante du service web orion (trafic non privilégié).

2. Descriptif des services internet

2.1. Service WEB (orion et liste verte)

Principe de la liste verte

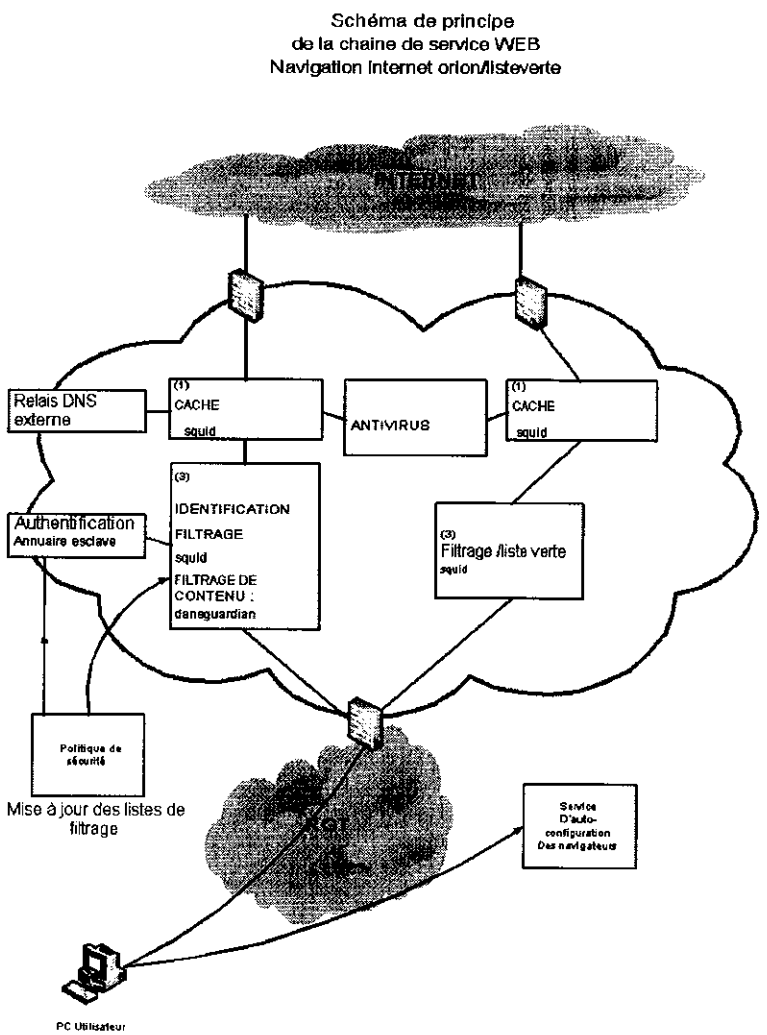
Permettre à l'ensemble des utilisateurs du Ministère d'accéder à des sites métiers et institutionnels de façon performante sur les réseaux externes publiques ou privés.

Principe d'orion

Chaque utilisateur dispose d'un compte personnel nominatif associé à un identifiant, un mot de passe, et un profil définissant ses droits d'accès au service. Un site intranet permet à chaque utilisateur de gérer son compte et de contrôler ses consommations.

Chaque Responsable de la Sécurité des Systèmes d'Information (RSSI) gère les comptes Orion de son entité sous l'autorité de son chef de service. Il dispose pour cela d'un accès au système d'information de la sécurité des systèmes d'information lui permettant de créer, modifier ou supprimer les comptes Orion de son entité et de gérer les profils associés. Il est chargé de faire appliquer les consignes d'utilisation définies par son chef de service.

Synoptique du service web



Politique de sécurité ORION

Fonctionnalités	Politique activée
Anti-virus	oui (coût de 40k€ initial et 2k€ annuel)
Filtrage de ports	Oui

Filtrage des urls et domaines	Liste fermée et listes noires
Filtrage d'adresses et d'extension	oui
Limitation de bande passante	oui
Limitation du nombre de connexions / client	Possible mais non activée
journalisation	oui
archivage	oui

Gestion des profils

Profil 1 :

Avec la mise en place de la nouvelle politique de filtrage Orion disparaissent les profils 1 qui ne représentaient plus que 1% des profils utilisateurs.

Ce profil était devenu obsolète et inutile car redondant avec le profil filtré (profil2). Tous les profils 1 existants ont été transformés en profils 2.

Profil 2 et 4 :

Ce profil de base ouvre l'accès à tous les sites référencés sur une liste fermée de domaines. La liste contient actuellement 50 mille sites. L'enrichissement de la liste fermée (ajout de sites à caractère professionnel et d'intérêt général) est possible en demandant l'ajout du ou des sites demandés.

Le profil 2-4 est conçu pour permettre une large diffusion de l'accès Internet au sein des services du Ministère de l'intérieur.

Profil 3 :

Ce profil donne accès à tous les sites autres que ceux répertoriés en liste noire. La liste noire comprend des sites hors du contexte professionnel ou pénalement répréhensibles.

Les blacklists (listes noires) contiennent des sites pouvant nuire à la sécurité du Ministère – virus, malware, spams, hameçonnage - ou pénalement répréhensibles.

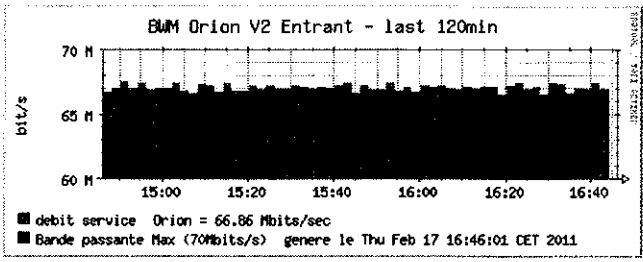
Exemples de journaux:

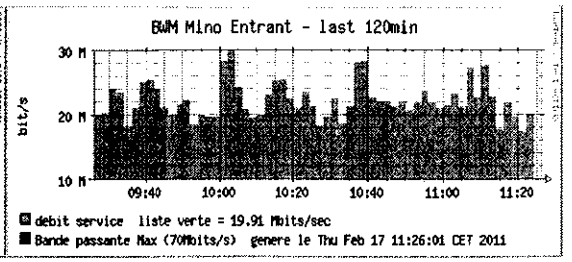
@ip - compte-orion [24/May/2011:00:05:19 +0200] "GET http://safebrowsing-cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAZYiY8DILCPAyoFr8cGAAMyCYnHAAD____Pw HTTP/1.0" 200 20283 TCP_MISS: FIRST_UP_PARENT

@ip - compte-orion [24/May/2011:00:05:19 +0200] "GET http://france.aprilia.com/assets/4466/showcase_sxv.jpg HTTP/1.0" 200 39941 TCP_MISS:FIRST_UP_PARENT
@ip - compte-orion [24/May/2011:00:05:19 +0200] "GET http://analytics.live.com/Sync.html? HTTP/1.0" 304 510 TCP_MISS:FIRST_UP_PARENT
@ip - compte-orion [24/May/2011:00:05:20 +0200] "GET http://clients1.google.fr/complete/search? HTTP/1.0" 200 610 TCP_MISS:FIRST_UP_PARENT
@ip - compte-orion [24/May/2011:00:05:20 +0200] "GET http://analytics.atdmt.com/Scripts/wlHelper.js? HTTP/1.0" 304 559 TCP_MISS:FIRST_UP_PARENT

Informations techniques

➢ Consommation de la bande passante environ 67 Mbits pour ORION et de 15 à 30Mbits pour la ListeVerte:





➢ Serveurs ORION:

Type de serveurs	Caractéristiques principales	nombre
cache	Espace disque	4
anti-virus	Puissance de traitement	4
Filtrage et identification	Taille de Ram et processeur	4
annuaire	aucune	2

Le ratio de cache est variable suivant les jours, il fluctue entre 20 et 40 % d'économie de bande passante.

➢ Serveurs LISTE VERTE:

Type de serveurs	Caractéristiques principales	nombre
cache	Espace disque	3
anti-virus	Puissance de traitement	3
Filtrage et identification	Taille de Ram et processeur	3

Le ratio de cache est variable suivant les jours, il fluctue entre 30 et 40 % d'économie de bande passante.

2.2. Service de messagerie internet

➢ Principe de fonctionnement

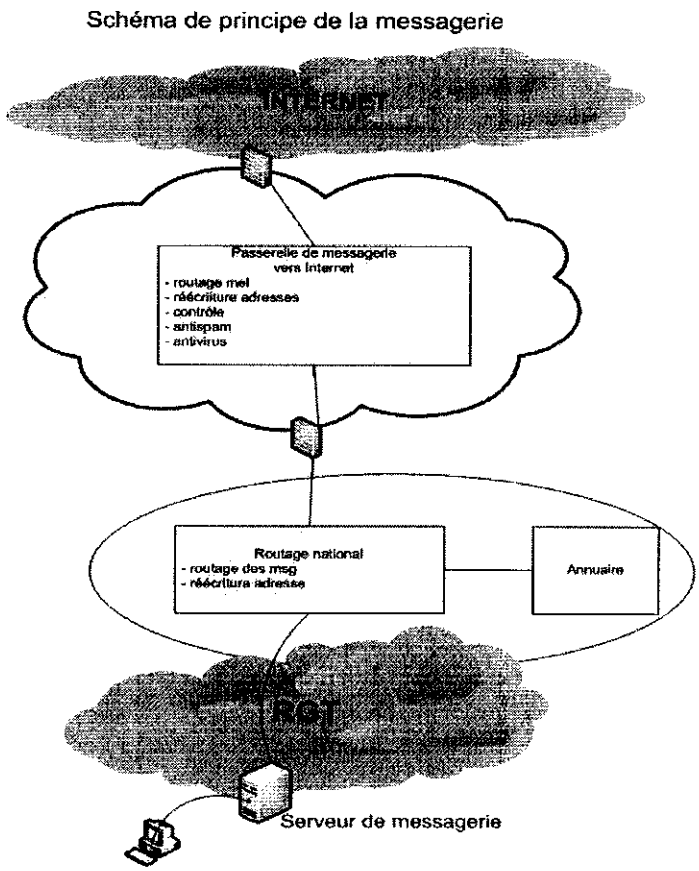
Les messages qui entrent et qui sortent sont soumis à des contrôles de sécurité de différentes natures afin de mettre en oeuvre la politique de sécurité définie en la matière:

Fonctionnalités	**Politique activée**
Anti-virus	oui (coût de 20k€ initial et 15k€ annuel)
anti-spam	Oui, marquage des mels en [!! SPAM]

greylisting	Oui
Filtrage d'adresses, d'extension	oui
Contrôles des entêtes SMTP	oui
journalisation	oui
archivage	oui

Les serveurs fonctionnent en haute disponibilité avec une charge de 20%.

➢ Schéma de principe



➢ Exemple de journaux

Jun 8 00:01:21 tigre postfix/smtpd[25780]: 1507312D80BD: client=exemple.fr[100.99.100.99]
Jun 8 00:01:21 tigre postfix/cleanup[26009]: 1507312D80BD: message-id=<xxxx@exemple.fr>
Jun 8 00:01:21 tigre6 postfix/qmgr[4121]: 1507312D80BD: from=exemple@exemple.fr, size=5755, nrcpt=1 (queue active)
Jun 8 00:01:21 tigre6 postfix/smtp[25518]: 1507312D80BD: to=<test@maine-et-loire.pref.gouv.fr>, orig_to=<test@maine-et-loire.gouv.fr>, relay=127.0.0.1[127.0.0.1]:26, delay=0.83, delays=0.74/0/0/0.09, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as BFEED25E063)

Description du service internet

du Ministère B

1. Présentation générale

Le Ministère B a centralisé et virtualisé les services de messagerie sur un datacenter en région parisienne. Les messages à destination d'internet sont routés vers la passerelle externe hébergée chez un prestataire. Ce ministère a également mis en oeuvre une architecture centralisée pour l'accès aux applications web. Cette architecture relaie les connexions web à destination de l'internet vers la plate-forme d'un prestataire de service qui gère les échanges web et messagerie avec internet.

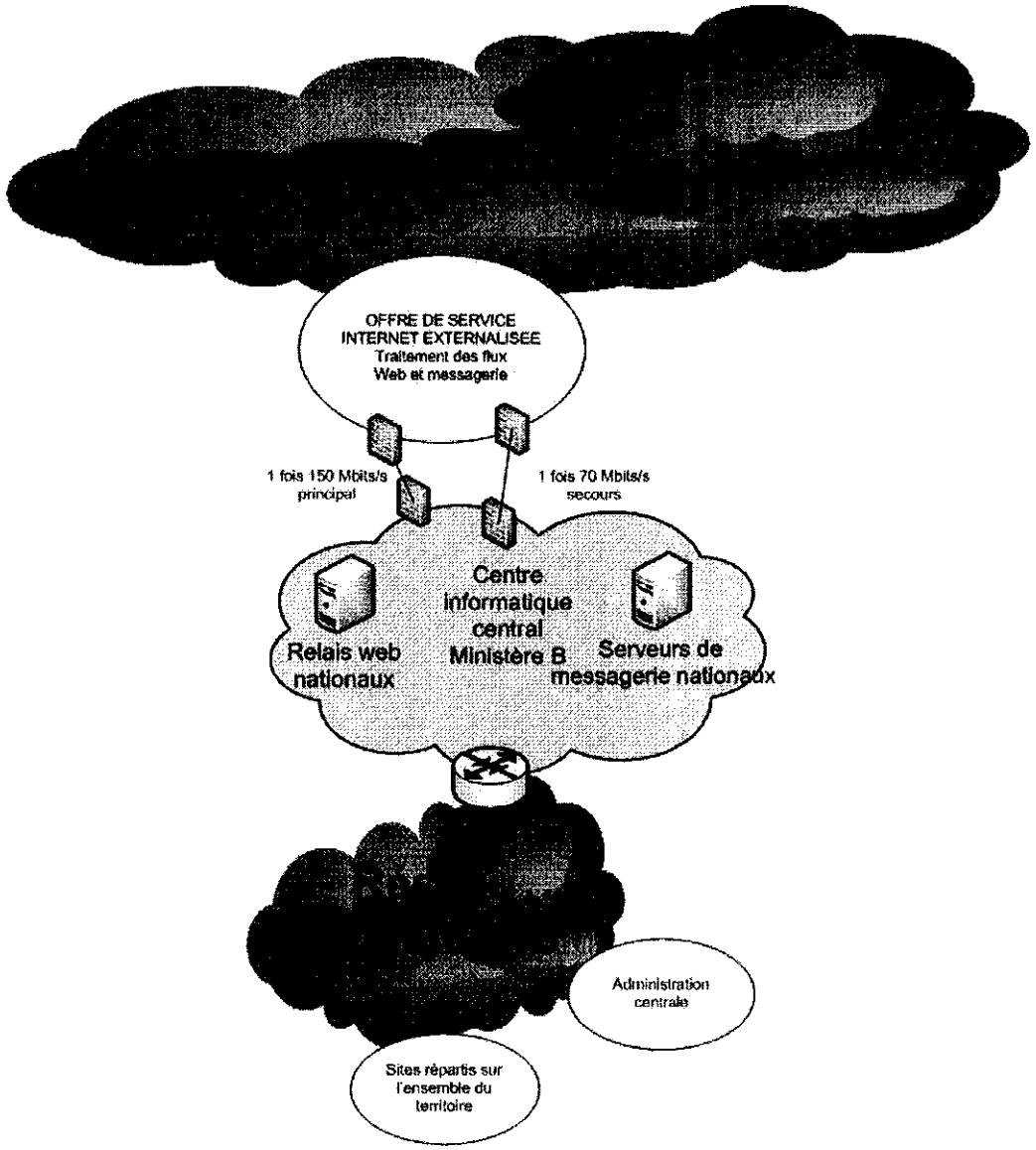
Le Ministère a publié sa politique de sécurité des systèmes d'information et a mis en place un réseau de RSSI. Le RSSI de la direction des opérations a validé la politique de sécurité appliquée par le prestataire au niveau de son offre de service. L'offre de service utilise des technologies qui ont fait l'objet de certification ou d'audit. Le prestataire est responsable de la prise en compte des préconisations de sécurité des éditeurs de systèmes et logiciels.

Le contrat de service prévoit une supervision H24 7j/7 de la disponibilité des services internet et un suivi mensuel sous la forme d'un tableau de bord standardisé.

Le coût de la prestation de service s'élève à 350 mille euros par an.

1.1. Schéma de principe

Le schéma ci-dessous représente l'architecture de principe des services d'accès à Internet pour le Ministère B.



1.2. Eléments quantitatifs

- service web: 100 mille clients ont accès au service de navigation web.
  - 80 millions de connexions par jour
  - le temps de réponse moyen du service n'est pas mesuré. Une majorité des clients trouvent que le service est suffisamment rapide.

- Messagerie : environ 100 mille adresses accessibles d'internet
  - 175 000 messages/jour entrants depuis internet (hors rejets)
  - 100 000 messages/jour sortants vers internet
  - 5 Mbits/s de débit entrant en moyenne entre 8h00 et 18h00

1.3. Ressources impactées par le service internet

Liste des différents acteurs du Ministère B impactés par le service internet:

- Le centre support qui gère les appels clients et ouvre les incidents auprès du prestataire.

- Les exploitants qui gèrent l'interface technique avec la plate-forme du prestataire (0,5 ETP).
- Les responsables de la sécurité des systèmes d'information du Ministère B.
- Le gestionnaire du contrat de service pour le Ministère B (0,5 ETP)

1.4. Accès internet

Le Ministère B utilise une offre de service assez ancienne qui consiste en un accès principal d'un débit de 150 Mbits/s et d'un accès secours d'un débit de 70 Mbits/s.

L'offre de service du prestataire permet de disposer d'un double accès actif/actif équilibré avec ou sans secours géographique moyennant un surcoût.

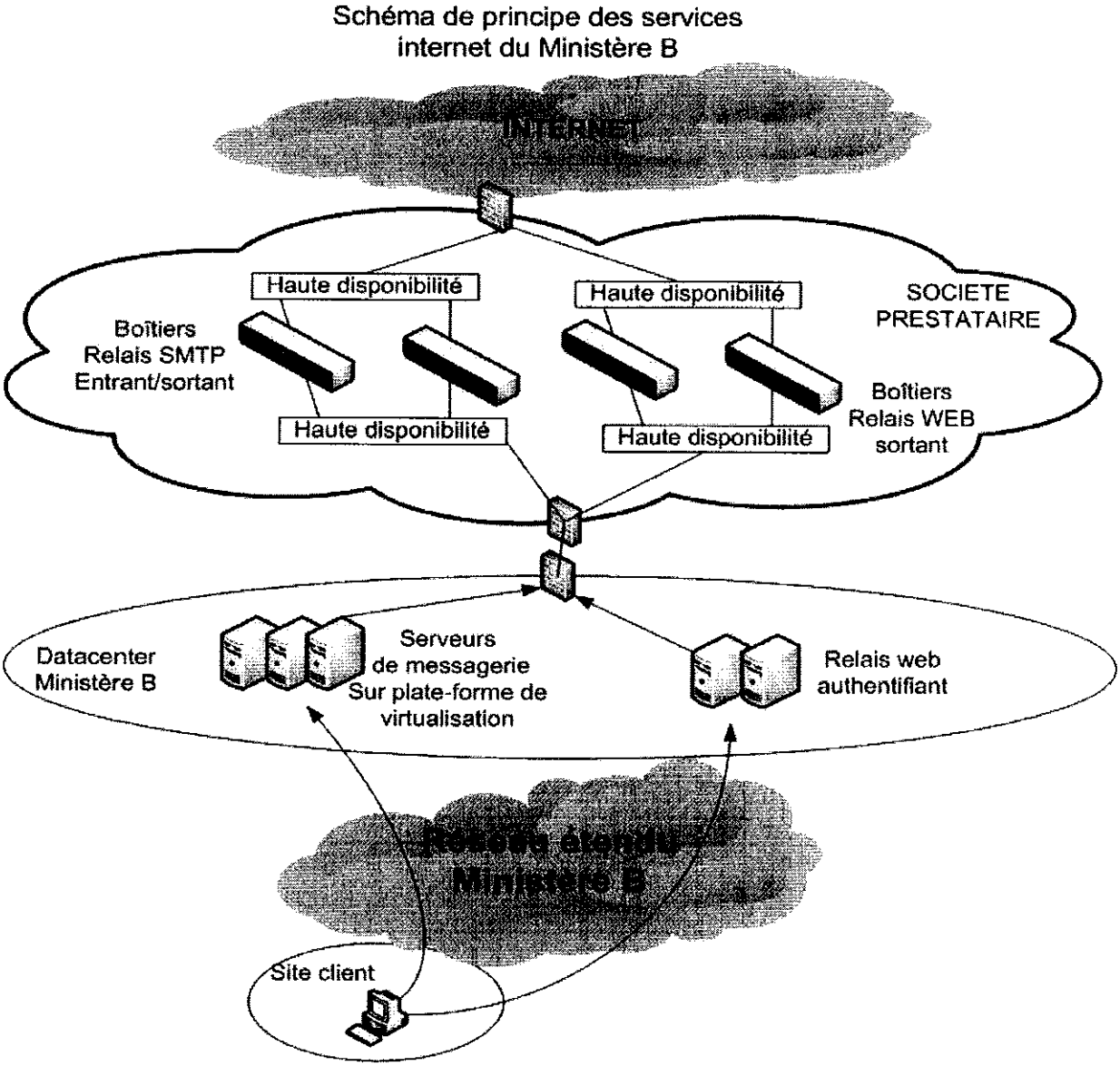
2. Description des services internet

2.1. Services WEB

➢ Fonctionnement

Les connexions internet vers les sites web métiers, gouvernementaux et les autres sont traitées par le même système. Le Ministère B adresse l'ensemble des requêtes web à destination d'internet vers la plate-forme du prestataire. Le traitement des requêtes est ensuite réalisé en fonction de la politique de sécurité définie avec le client.

➢ Schéma de principe



➢ Informations techniques

La solution du prestataire est basée sur des boîtiers de filtrage d'URL IronPort S660 fonctionnant en haute disponibilité. Un cluster de répartiteurs de charge permet d'assurer la haute-disponibilité du service et de faire évoluer l'offre en termes de performances. Pour augmenter les performances du service ou le nombre d'utilisateurs du service, il suffit de rajouter un boîtier S660 derrière un des répartiteurs de charge.

Le proxy IronPort Série S fonctionne en mode explicite dans le cas présent. Le moteur proxy supporte les flux HTTP (toutes versions), HTTPS, FTP encapsulé dans du HTTP et peut également servir de relais sur tout flux compatible avec le rejeu d'une connexion TCP (TCP CONNECT).
IronPort embarque une solution de filtrage URL par catégorie, qui sera alors utilisée pour gérer les accès Internet des employés, en autorisant, limitant ou bloquant les accès aux sites en fonction de leur catégorie.
Ces solutions de filtrage URL par catégorie permettent aussi de bloquer les accès aux sites connus de phishing ou connus pour être infectés par du malware et catégorisés comme tels. Il est possible

avec le boîtier Série S de définir des groupes, soit par sous-domaine, soit par groupe LDAP en allant interroger l'annuaire LDAP de l'entreprise, et d'affecter à chaque groupe une politique distincte en ce qui concerne chacun des filtres qui viennent d'être décrits : filtres URL par catégorie, filtres de réputation Web, moteur anti-malware, contrôle des applications, analyse du contenu Web.

Modes de connexion
Il existe deux modes de connexion :
mode Invité : avec ce mode de connexion, les utilisateurs n'ont pas besoin de s'authentifier pour se connecter à Internet ;
mode Identifiant : avec ce mode, les utilisateurs souhaitant se connecter à Internet doivent s'identifier. Ce mode permet d'obtenir des informations nominatives d'un utilisateur identifié.

Le ministère B a choisi le mode invité.

Protocoles
IronPort Serie S est un serveur proxy jouant le rôle de passerelle entre le réseau du client et Internet. Lorsqu'un ordinateur client lance une requête pour obtenir un document, il demande à l'IronPort de récupérer le document, plutôt que de le récupérer lui-même. IronPort prend en charge les protocoles HTTP (HyperText Transfer Protocol), HTTPS (HyperText Transfer Protocol Secure) et FTP (File Transfer Protocol).

Listes de filtres
Il existe 2 types de listes :

- listes de filtres prédéfinies : le boîtier IronPort Série S inclut une base de catégories d'URL embarquée. Cette base contient 52 catégories prédéfinies et plus de 21 millions de sites Internet. Elle est mise à jour automatiquement et de façon régulière sur les boîtiers.
- listes de filtres locales : un administrateur du client peut également créer ses propres listes de filtres locales pour ajouter des URLs. Lorsque l'accès à Internet est demandé, l'IronPort vérifie les listes de filtres locales avant ses listes prédéfinies. Si IronPort détecte une correspondance dans une ou plusieurs listes locales actives, il n'effectue pas de contrôle dans les listes prédéfinies d'IronPort.

Le réseau de RSSI du ministère B recueille les signalements des utilisateurs concernant les erreurs de filtrages et les transmets via le gestionnaire du contrat de service au support du prestataire. Il n'y a pas de liste de filtres locales.

Système anti-malware / anti-virus
IronPort propose un filtrage à base de signatures au niveau de la passerelle afin d'éviter les problèmes de latence. Pour ce faire, il utilise son système anti-malware, piloté par le moteur IronPort DVS (Digital Vectoring & Streaming), qui va lancer de manière simultanée un certain nombre d'analyses sur les données ou flux.
Ce système d'analyse présente deux innovations majeures :
la Série S embarque aujourd'hui le moteur anti-malware de Webroot et le moteur anti-virus de McAfee. L'utilisation conjointe et simultanée de plusieurs moteurs permet une plus grande couverture des risques.
L'analyse des objets Web est faite à la volée, en mode streaming, ce qui permet un confort utilisateur et une minimisation des temps de latence. En effet le scan commence en même temps que le téléchargement de l'objet, et si un code malveillant est identifié, le téléchargement est immédiatement stoppé, ce qui améliore de façon sensible la capacité de traitement du boîtier.

L'analyse des contenus Web et des fichiers
Le moteur d'analyse peut effectuer une analyse des contenus Web et ainsi :

- limiter la taille des objets Web téléchargés
- bloquer les téléchargements d'objets Web en fonction de leur nature (MP3, vidéo, etc.)

L'accès à des documents peut être bloqué en fonction de leur extension, de leur type de média ou de leur nombre magique. L'administrateur d'un client peut, par exemple, empêcher les utilisateurs de télécharger des fichiers "mp3" ou "audio/mpeg".

Le ministère B a renoncé à limiter la taille des objets mais a fait activer le filtrage de contenu vidéo et musique.

2.2. Relais de messagerie internet

➢ fonctionnalités

Un relais de messagerie SMTP dédié assure l'interface entre les serveurs de messagerie du client et l'internet public (SMTP entrant et sortant).
Les fonctionnalités actives du service de messagerie internet sont :

- détection antivirus double
- détection antispam (incluant anti-phishing et malware)
- filtrage de contenu
- mise en quarantaine utilisateur
- interfaces web d'administration pour le client
- notification journalière des utilisateurs listant les mails en quarantaine
- rapports

La solution répond aux exigences suivantes :

- un service avec un taux de disponibilité de 99,95% sur les serveurs gérés
- un service entièrement managé par le prestataire comprenant l'administration, l'exploitation, la maintenance ainsi que la supervision du service en 24 x 7 x 365.
- un service sécurisé : la mise à jour des signatures des anti-virus et de l'anti spam est effectuée automatiquement.
- un Web Service Client pour les administrateurs permettant la création/modification et la consultation des statistiques du service.

➢ Traitement des messages

Les serveurs relais de la plate-forme du prestataire gèrent le trafic entrant et sortant avec Internet. Le trafic est réparti entre les serveurs via les répartiteurs de charge. Les serveurs relais appliquent les politiques de sécurité entrante et sortante du client et en fonction du résultat des tests les messages sont acceptés, rejetés ou mis en quarantaine.

➢ Politique de Sécurité

Deux politiques de sécurité sont implémentées:

- Une politique de sécurité qui est appliquée au niveau de la connexion SMTP. Elle est gérée par la solution ironPort qui analyse des éléments de la connexion SMTP comme l'adresse source IP du serveur demandant la connexion, le domaine de l'émetteur, etc. et en fonction des filtres accepte ou rejette la connexion.
- Une politique de sécurité qui est appliquée après que la connexion SMTP a été acceptée. Elle est gérée par la solution qui analyse le message lui-même (vérification antivirus, antispam etc. ...) en appliquant la politique de sécurité correspondante. Le message est

alors accepté, détruit, mis en quarantaine ou marqué et des actions associées comme une notification peuvent être lancées parallèlement.

Les caractéristiques des politiques de sécurité sont :

- La politique de sécurité est différente suivant que le message est entrant (venant d'internet) ou sortant
- La quarantaine IronPort est un espace sécurisé qui conserve les messages suspects (spam par exemple) jusqu'à ce qu'un administrateur client ou un utilisateur effectue une action (récupération, destruction)
- Les messages en quarantaine sont automatiquement détruits après 4 semaines.

➢ Service de filtrage

Le service de filtrage inclut toutes les fonctions liées au filtrage aussi bien au niveau réseau qu'au niveau applicatif.

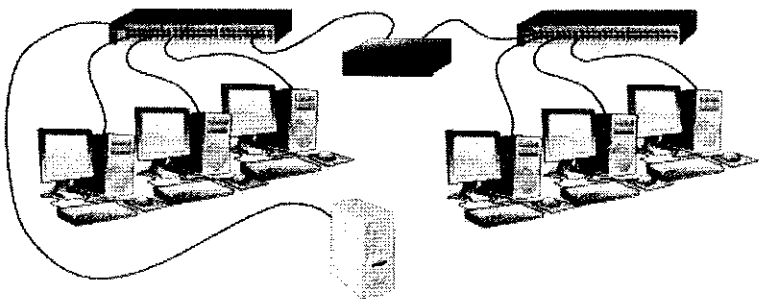
➢ Fonctionnalité anti-spam

Le moteur antispam applique ses filtres sur les différentes parties du message (émetteur, destinataires, adresse Ips, URIs, numéro de téléphone etc. ...).

➢ Fonctionnalité anti-virus

La solution comporte deux moteurs anti-virus en série (Mcafee et Sophos) qui vérifient en temps réel tout message qui passe par les serveurs relais. Il bloque les virus, les vers et toutes les menaces qui combinent spam et attaque « DoS » (déni de service).

Le serveur mandataire



Nous travaillons ici au niveau 4 (du modèle DOD) c'est à dire au niveau du protocole d'application (HTTP pour ce qui nous concerne ici). Il existe deux types de serveurs mandataires :

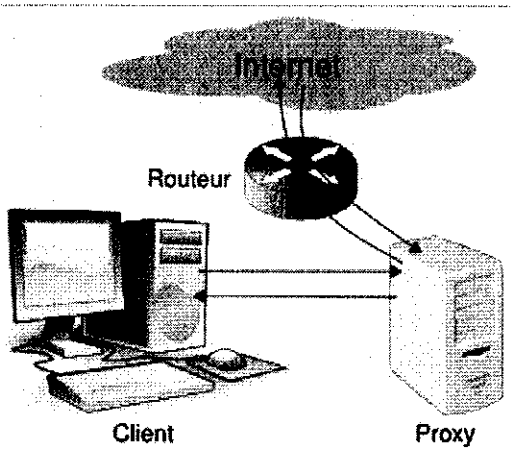
- Le proxy « normal », qui nécessite que l'application cliente sache que le proxy existe et sache aussi travailler avec. En effet, dans ce cas, le client envoie ses requêtes au serveur mandataire, à charge pour lui d'aller chercher plus loin l'information réclamée par le client et de la lui transmettre, une fois l'information obtenue. Les clients HTTP (navigateurs) modernes savent tous le faire. C'est en revanche très rarement le cas pour d'autres protocoles comme POP, FTP etc ;

Objectif

Installer un système de proxy cache pour HTTP. Ce proxy-cache propose deux fonctions principales :

- L'optimisation de la bande passante sur le lien Internet, lorsque de nombreux clients sont connectés et qu'ils visitent plus ou moins les mêmes sites, à la condition, bien sûr, que ces sites ne soient pas trop dynamiques, ASP, JSP, PHP... ni chiffrés (HTTPS). Comme vous le constatez, la fonction cache présente de moins en moins d'intérêt. Il en reste un cependant, surtout pour les illustrations qui ne sont pas encore toutes en flash ;
- le contrôle et le filtrage de l'accès à la toile, en se servant des URI et, éventuellement, des noms d'utilisateurs, si l'on fait de l'authentification de ces derniers, autant de choses qu'il est difficile, voire impossible de faire avec du filtrage de paquets. En effet, en travaillant au niveau du protocole HTTP, il devient possible de mettre en place des filtres d'URI, des analyses de contenu dans les documents, alors qu'au niveau IP, nous ne pourrions filtrer que sur des adresses et des ports.

Tout responsable d'un réseau local à l'usage de mineurs et connecté à l'Internet se doit de mettre en place un tel système de filtrage de manière à éviter, autant que possible, l'accès à des sites que la morale réprouve, d'autant qu'il s'agit d'une obligation légale.



Dans le cas d'un proxy « normal », le client demande au proxy d'interroger le serveur cible. Ce dernier répond au proxy qui communique alors la réponse au client. Dans ce mode, le client est configuré pour utiliser un proxy et il modifie les requêtes http en fonction.

Le logiciel

Squid, principal composant de ce système, assure les fonctions de :

- Cache, pour optimiser la bande passante ;
- identification des utilisateurs, nous en verrons une simpliste et une nettement plus complexe ;
- filtrage d'accès « basique », mais déjà intéressant.

SquidGuard propose un filtrage très puissant d'accès au web, en fonction :

- De groupes d'utilisateurs, définis de diverses manières. Ici, nous nous baserons sur des IPs ou des groupes d'IPs, mais il est possible d'utiliser l'identification des utilisateurs mise en place sur Squid ;
- de listes de domaines et d'URI qui serviront à définir soit des cibles autorisées, soit des cibles interdites (listes blanches, listes noires) ;
- de plages horaires pendant lesquelles l'accès sera autorisé ou interdit

Et bien d'autres choses encore, que nous ne verrons pas ici.

Description des moyens de lutte contre le spam
(site messagerie.dsic.mi et site http://www.radical-spam.org)

Outil de filtrages des courriels indésirables

L'outil de filtrage des courriers indésirables fait partie des équipements de sécurité des passerelles de messagerie du ministère. Le produit utilisé est celui de la société Kaspersky

Méthodes d'analyse

Cette solution combine plusieurs méthodes de détection :

- listes noires (adresses électroniques et domaines notoirement générateurs de spam) qui sont mises à jour en ligne
- analyse du contenu : comparaison des textes avec des exemples prédéfinis
- analyse du contenu : recherche intelligente selon des termes et mots-clés prédéfinis
- reconnaissance de caractères pour filtrer les textes "masqués" dans des images

L'analyse de contenu s'appuie sur des exemples de spams et une liste de mots clés **mis à jour automatiquement et très fréquemment**. Cette mise à jour s'effectue à partir d'un très grand nombre de machines réparties sur l'ensemble du réseau Internet.

Méthodes de traitement

Le filtrage antispam s'effectue sur les passerelles de messagerie du ministère. Il s'applique à **tous les mails en provenance d'Internet**. Pour des raisons évidentes, nous ne filtrons pas les messages internes, ni les messages en provenance des autres administrations.

Aucun message n'est supprimé. Si un message est détecté comme un spam, il n'est pas détruit mais simplement marqué. L'objet du message est alors modifié et un champ dans l'en-tête est ajouté selon la probabilité que la détection soit bonne :

Une protection préliminaire est appliquée via le greylisting:

Article – Le Greylisting (La liste grise)

Lorsque votre passerelle reçoit un message, elle dispose entre autre de 3 informations essentielles :

- L'adresse IP du client emetteur
- L'adresse email de l'expéditeur
- L'adresse email du destinataire

Ces 3 informations constituent ce que l'on appelle un triplet.
Grâce à ces triplets vous allez pouvoir alimenter une base de données, sous la forme d'un fichier plat, une base au format Berkeley ou une base SQL.

Pour comprendre l'interêt de la liste grise et ses limites, il faut comprendre le mode opératoire de beaucoup de spammeurs :

1. Constitution d'un fichier de plusieurs millions d'adresses email pour un envoi de masse ou utilisation d'un fichier existant
2. Utilisation d'un programme d'envoi existant ou développement d'un programme spécifique
3. Recherches des enregistrement MX pour tous les domaines correspondants aux adresses emails référencées
4. Début de l'envoi du spam
5. Pour chaque mail envoyé, mettre à jour l'enregistrement dans la base pour savoir si le message à bien été accepté
6. **Si le message est refusé, passer au suivant**

C'est la dernière ligne, ci-dessus qui donne de l'interêt au système de liste grise car le message va systématiquement être refusé au moins une fois pour chaque triplet.

signal spam

COMMUNIQUE DE PRESSE

Face à l'augmentation de la fraude sur Internet,

l'OCLCTIC et Signal Spam signent une convention de partenariat

Paris, le 4 mai 2011

Valérie Maldonado, commissaire divisionnaire, chef de l'**office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire (DCPJ),** et **Jean-Christophe Le Toquin,** président de l'association Signal Spam, le réseau de confiance pour agir contre le spam, ont **signé** le **mercredi 4 mai 2011** une **convention de partenariat** s'inscrivant dans le cadre de la lutte contre le spam, véhiculant fraudes et escroqueries, et pour un Internet plus sûr.

Cette signature officialise un partenariat public-privé débuté en 2005 et formalise l'optimisation des dispositifs mis au service des internautes tout autant que l'efficacité des actions contre le spam et les spammeurs. Projet unique au monde réunissant tous les acteurs de l'écosystème email : entreprises et opérateurs, associations et acteurs publics, Signal Spam repose sur le signalement par les internautes des courriels de toute nature dont ils s'estiment victimes, et ce, en toute simplicité.

S'appuyer sur la richesse des partenariats pour encore plus d'efficacité

Trois ans après la création de la plateforme nationale de signalement des contenus illicites de l'Internet (www.internet-signalement.gouv.fr), les états statistiques montrent la persistance de ces pratiques délictuelles lucratives. Si en 2009, la plateforme dénommée « PHAROS » a reçu 52.353 signalements, dont 50,6 % se rapportant à des escroqueries, en 2010 ce sont 77.646 signalements qui ont été reçus, dont 57% relatifs aux escroqueries. Pour 2011, si la tendance des trois premiers mois se poursuit, la barre des 100 000 signalements pourrait être atteinte à la fin de l'année, dont une moitié pour les escroqueries.

Optimiser les flux de signalement en combinant les compétences

Pour Valérie Maldonado, *« c'est dans un esprit d'efficacité dans le plan de lutte commun contre le spam que le directeur général de la police nationale a émis un avis favorable à la signature de cette convention. Elle assure un rapprochement judicieux entre la plateforme PHAROS et celle de Signal Spam. A cet égard, une redirection vers Signal Spam est maintenant proposée à l'internaute dans le formulaire de signalements PHAROS lorsqu'il sélectionne « spam » dans la liste des infractions. Signal*

Spam étant la structure la mieux à même de traiter et d'analyser les spams dans l'intégralité de sa problématique. »

Lutter efficacement en prenant le problème du spam à la source

Les informations transmises à Signal Spam par les internautes sont relayées vers les acteurs concernés, publics et privés, afin qu'ils agissent à la source de l'envoi. Désinscription dans les listes marketing par les routeurs et les annonceurs, contrôles par la CNIL des entreprises aux pratiques abusives, neutralisation par les fournisseurs d'accès Internet des ordinateurs infectés et utilisés dans des réseaux d'envoi de spams (botnet), sont quelques-unes des actions possibles. Cette base de signalements constitue également une source de preuves lors d'enquêtes judiciaires menées par les services de police et de gendarmerie. Jean-Christophe Le Toquin, président de l'association Signal Spam : *« Cette convention est une nouvelle avancée dans la mobilisation concertée des acteurs publics et privés. Elle assure la possibilité de lutter sur tous les fronts afin d'assainir les réseaux et de préserver la confiance des internautes dans l'usage de l'email. Signaler, c'est agir ».*

Contacts presse

Direction générale de la police nationale
Service d'information et de communication
de la police nationale (SICoP)
Tel : 01 40 07 60 70
sicopmedia@interieur.gouv.fr

Jérôme Granger, en charge des relations publiques de Signal Spam
jerome.granger@signalspam.net

Vick Hayford, vice-président de Signal Spam
en charge du comité opérationnel
vick.hayford@signalspam.net

Les membres Signal Spam

Institutionnels : CNIL, ANSSI, OCLCTIC, DGGN, BEFTI - ***Associations*** : AFA, AFOM, BSA, FEVAD, SNCD, UDA - ***Associations internationales*** : MAAWG, NCFTA Canada - ***Entreprises « Membres fondateurs »*** : Microsoft, SFR, Orange, NP6 MailPerformance, Experian CheetahMail, Come&Stay - ***Entreprises*** : eBay/Paypal, Lexsi, Vade Retro Technologies, G Data Software, Return Path, Atos Worldline, Emailvision, eCircle, Alinto, Cloudmark, Splio

SOURCE : http://www.squid-cache.org

Communication between browsers and Squid

Most web browsers available today support proxying and are easily configured to use a Squid server as a proxy. Some browsers support advanced features such as lists of domains or URL patterns that shouldn't be fetched through the proxy, or JavaScript automatic proxy configuration.

There are three ways to configure browsers to use Squid. The first method involves manually configuring the proxy in each browser. Alternatively, a proxy.pac file can be manually entered into each browser so that it will download the proxy settings (partial auto configuration), and lastly all modern browsers can also and indeed are configured by default to fully automatically configure themselves if the network is configured to support this.

Recommended network configuration

For best use of the proxy we recommend a multiple-layers approach. The following are the layers we recommend, in order of preference.

We are aware that many networks only implement layer 3 and 4 of this design due to administrators familiarity with NAT, confusion about the benefits, and historic problems with the upper two layers.

1. Web Proxy Automatic Detection (**WPAD**) (aka **transparent configuration**)
    - Browsers set to auto-detect the proxy for whatever network they are plugged into. This is particularly useful for mobile users.
    - The big problem with this layer is that there is no formal RFC standard to follow, so browsers implement and two separate DNS and DHCP systems to setup.
    - requires the PAC to be implemented.
2. Proxy auto-configuration (**PAC**) (aka *transparent proxy*)
    - As a backup to per-machine configuration.
    - Some systems support PAC file to be explicitly set in the machine-wide environment.
3. Machine-wide Configuration
    - Using a system-wide environment variable **http_proxy** (or GUI configuration which sets it). Most operating systems support this. Windows is the exception, however the IE settings are used in an equivalent way.
    - A lot of software supports it. Only set once per machine.
    - Some systems allow this to be pushed out across the network (Windows uses a Domain Policy)
4. NAT or TPROXY interception. (aka *transparent proxy*)
    - Client software does not need to be touched.
    - security takes several major reductions (several whole families of vulnerability are created, proxy authentication disappears)
    - System resources and connection reliability take several major reductions
5. Manual Configuration.
    - Nothing beats an explicit manual configuration for *it works* excitement. However doing it for each and every piece of software on a machine is quite a hassle. Doing it for a whole network is unrealistic outside of highly paranoid systems. It is mentioned here simply as an option.

For completeness sake: the best underlying secure systems back several of these layers up with a complete firewall ban on web traffic. This prevents users and machines bypassing the proxy control points.

Partially Automatic Configuration

This involves the browser being preconfigured with the location of an autoconfiguration script.

Netscape automatic configuration

Netscape Navigator's proxy configuration can be automated with JavaScript (for Navigator versions 2.0 or higher). Select **Network Preferences** from the **Options** menu. On the **Proxies** page, click the radio button next to **Automatic Proxy Configuration** and then fill in the URL for your JavaScript proxy configuration file in the text box. The box is too small, but the text will scroll to the r8ight as you go.

Microsoft Internet Explorer

Microsoft Internet Explorer, versions 4.0 and above, supports JavaScript automatic proxy configuration in a Netscape-compatible way. Just select **Options** from the **View** menu. Click on the **Advanced** tab. In the lower left-hand corner, click on the **Automatic Configuration** button. Fill in the URL for your JavaScript file in the dialog box it presents you. Then exit MSIE and restart it for the changes to take effect. MSIE will reload the JavaScript file every time it starts.

Redundant Proxy Auto-Configuration

by Rodney van den Oever

There's one nasty side-effect to using auto-proxy scripts: if you start the web browser it will try and load the auto-proxy-script.

If your script isn't available either because the web server hosting the script is down or your workstation can't reach the web server (e.g. because you're working off-line with your notebook and just want to read a previously saved HTML-file) you'll get different errors depending on the browser you use.

The Netscape browser will just return an error after a timeout (after that it tries to find the site 'www.proxy.com' if the script you use is called 'proxy.pac').

The Microsoft Internet Explorer on the other hand won't even start, no window displays, only after about 1 minute it'll display a window asking you to go on with/without proxy configuration.

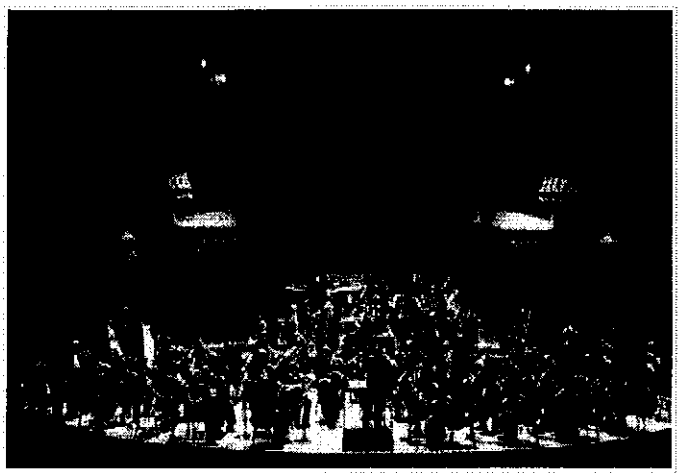
The point is that your workstations always need to locate the proxy-script. I created some extra redundancy by hosting the script on two web servers (actually Apache web servers on the proxy servers themselves) and adding the following records to my primary nameserver:

```
proxy   IN      A       192.0.2.1 ; IP address of proxy1
        IN      A       192.0.2.2 ; IP address of proxy2
```

The clients just refer to 'http://proxy/proxy.pac'. This script looks like this:

```
 1 function FindProxyForURL(url,host)
 2 {
 3 // Hostname without domainname or host within our own domain?
 4 // Try them directly:
 5 // http://www.domain.com actually lives before the firewall, so
 6 // make an exception:
 7 if ((isPlainHostName(host)||dnsDomainIs( host,".domain.com")) &&
 8         !localHostOrDomainIs(host, "www.domain.com"))
 9         return "DIRECT";
10
11 // First try proxy1 then proxy2. One server mostly caches '.com'
12 // to make sure both servers are not
13 // caching the same data in the normal situation. The other
14 // server caches the other domains normally.
15 // If one of 'm is down the client will try the other server.
16 else if (shExpMatch(host, "*.com"))
17         return "PROXY proxy1.domain.com:8080; PROXY proxy2.domain.com:8081;
DIRECT";
   18  return  "PROXY  proxy2.domain.com:8081;  PROXY  proxy1.domain.com:8080;
DIRECT";
19 }
20
```

I made sure every client domain has the appropriate 'proxy' entry. The clients are automatically configured with two nameservers using DHCP.

ISO 22301 : la future norme de Continuité d'activité

L'organisme international de normalisation ISO, après avoir travaillé le texte d'une proposition de norme pour la Continuité d'activité, vient de le soumettre au vote de ses membres.

Une nouvelle norme va donc normalement voir le jour fin avril 2011 date du dépouillement. Son titre : "Sécurité sociétale — État de préparation et systèmes de gestion de la continuité — Exigences".

Ce genre de norme est important pour au moins deux raisons :

- son adoption par l'entreprise indique clairement une intention d'amélioration inscrite dans la durée en matière de continuité
- les partenaires de l'entreprise -client ou fournisseurs- savent que des mesures sont en place et que l'entreprise présente un niveau de risque et un degré de préparation face au sinistre meilleurs que d'autres.

Voici nos premières remarques.

C'est une norme "système de gestion"

Cette norme appartient à une catégorie bien particulière : les "management systems" ou "systèmes de gestion". Cela signifie qu'elle se concentre sur la manière de se rapprocher d'un état cible.

Autrement dit, elle présente des dispositifs à mettre en place pour permettre d'améliorer la situation en matière de continuité d'activité. Ce type de norme s'appesantit beaucoup plus sur le fait de se rapprocher d'une cible de bonnes pratiques que sur les bonnes pratiques elles-même. Ceux qui y recherchent des "recettes" en seront pour leurs frais.

En ce qui concerne les bonnes pratiques (à chercher à atteindre) il faut se référer à un autre corpus, normé ou pas d'ailleurs.

On peut très bien faire l'analogie avec les normes de sécurité de la famille ISO 27000 ou de qualité ISO 9000 qui possèdent en leur sein une norme "système de gestion". Ces normes "de gestion" présentent toutes une même caractéristique : l'engagement nécessaire de la Direction générale.

Elles responsabilisent la Direction générale (DG) : elles ne disent pas "voilà ce qu'il faut faire en matière de continuité" mais "la DG doit choisir ce qu'elle veut en matière de continuité". C'est ce que ces normes appellent "une politique de continuité". (On peut remplacer dans ce qui précède 'continuité' par 'sécurité' ou 'qualité', selon la norme.)

Pour réaliser ces choix de niveau stratégique, des recommandations sont faites dans la norme, qui énonce quelques critères. Il est clair cependant qu'un travail de préparation est à faire en amont, en général accompagné et suscité par un responsable (RPCA dans ce cas).

Nous voyons souvent dans nos missions de conseil ce document de politique rédigé quelques mois après la nomination du RPCA et sous l'impulsion de ce dernier. L'analogie avec la qualité et la sécurité demeure.

Où l'on retrouve le célèbre PDCA ou cycle de Deming

Conséquence probable de ce qui précède et d'un réalisme tout anglo-saxon, ce type de norme envisage un progrès avec le temps.

Elles s'inscrivent en effet dans un cycle d'amélioration : réalistes, elles considèrent qu'il faut commencer en mettant la barre assez bas puis la monter progressivement. Dit autrement, elles ne sont pas binaires ('bien' / 'mal') mais beaucoup plus dosées ('moyen' / 'mieux l'année prochaine').

C'est le fameux PDCA (Plan Do Check Act):
- P : Plan ou prévoyez ce que vous voulez faire pour la période N°n
- D : Do ou faites-le, passez à l'acte : cela se traduit par des plans d'actions divers qui permettent d'améliorer la situation
- C : Check : faites des essais, des exercices, vérifiez ce qui marche ou pas.
- A : Pour ce qui ne marche pas, ré-agissez par des corrections

Enfin, recommencez en haut de la liste à la lettre P avec n+1.

C'est une norme "comminatoire"

Nous l'avons vu, il existe des normes de 'bonnes pratiques' et des normes 'système de gestion'.

Les normes de bonnes pratiques listent un certain nombre de recommandations intéressantes classées logiquement. Le verbe employé en anglais est "should", les quelques traductions en français spécifient "il convient". On peut donc en prendre et en laisser.

Les normes de système de gestion sont plus exigeantes, elles précisent 'you shall' ou 'il faut'. En particulier elles demandent que la DG choisisse ce qu'elle prend ou laisse dans le corpus de bonnes pratiques. Cela amène à des obligations qui peuvent faire sourire : "la politique est faite pour être appliquée" ou sembler évidentes.

La conséquence directe de cet état de fait est qu'il devient possible de savoir si la norme 'système de gestion' est suivie ou non. "Il faut faire ceci" stipule la norme : "est-ce fait ?" peut demander l'auditeur "oui" ou "non" sont des réponses possibles. Ce type de norme peut donc faire l'objet d'un certification. Des certifications ISO 22301 pourraient donc apparaître ultérieurement.

Une norme 'système de gestion' se prête, comme on le voit, à des mécanismes de certification alors qu'une norme 'bonnes pratiques' ne s'y prête pas. L'ISO 22301 mentionne d'ailleurs des possibilités d'auto-évaluation ou d'audit par des tiers intéressantes car ouvrant la porte à des certifications plus souples.

L'exigence première et fondatrice est que la Direction générale doit commencer par dire ce qu'elle veut faire en matière de continuité dans tel ou tel corpus de bonnes pratiques, attribuer des responsabilités dans son organisation et suivre ce qui est fait pour corriger. Elle doit aussi prévoir le nécessaire en matière de support, d'assistance compétente et de traitement des difficultés.

Ce document de "politique de continuité" doit exister avant tout. Il doit être largement communiqué dans l'entreprise et auprès de ceux que cela concerne hors entreprise : c'est la première exigence de la norme.

Et la Continuité dans tout cela ?

En gros ce qui précède est valable pour toute norme 'système de management' ; qu'est-il exigé spécifiquement en matière de continuité d'activité dans cette future norme ISO 22301 ?

Les points détaillés se résument à ce qui suit :

- Il faut cadrer l'approche : définir le périmètre sur lequel le système de gestion va porter ; tout bon chef de projet sait qu'il faut commencer par là...

- Il faut mener une **analyse de risque** et un **BIA (Business Impact Analysis)** ; il est amusant de voir ces deux analyses rassemblées dans le même paragraphe quand on sait que l'approche britannique met le BIA en premier alors que l'approche US commence par l'analyse de risque. La norme -c'est normal pour un système de gestion- ne dit pas comment faire cela, mais se contente de préciser des points durs comme la nécessité d'avoir des critères d'évaluation et des méthodes pour les risques ou la détermination des activités critiques de l'entreprise ainsi que des délais d'interruption maximum admissibles.

- Il faut déterminer et choisir les options de continuité : les activités prioritaires et les ressources sous-jacentes (humaines, techniques, informatiques, locaux, bureaux, etc.) à prévoir ; quant aux risques, il faut prévoir d'en diminuer les effets et occurrences...

- Il faut mettre en place la réponse appropriée : les procédures et l'organisation qui permettent de redémarrer dans le contexte du sinistre au-delà d'un certain seuil de gravité ; il faut y inclure la communication vers les parties-prenantes. Les missions et responsabilités doivent être décrites.

- Il faut mettre en place des procédures de surveillance, d'alerte en cas de sinistre et de mise en place de la

réponse.

- Il faut construire des "Business Continuity Plans" comprenant un certain nombre de points traditionnels de la discipline et penser aussi au retour à la normale quand tout est rentré dans l'ordre.

- Il faut faire des exercices et des tests pour s'assurer que les procédures conviennent et répondent aux objectifs de continuité.

- Il faut prévoir des audits et des revues régulières, la direction générale doit s'assurer de l'efficacité des procédures et plans en place.

- Enfin, PDCA oblige, il faut mettre en place et vérifier les actions correctives face aux anomalies constatées.

Des exigences minimales mais structurantes

Chacun de ces points est traité sur une page ou deux tout au plus, ce qui porte à 12 le nombre de pages spécifiant les exigences propres à la continuité d'activité sur un document comptant 32 pages.

Il est possible de sentir des "redites" dans les phrases de la norme, indiquant des sources multiples (comme le British Standard et le DRII nord-américain, entre autres).

L'ensemble de ces exigences est évidemment structurant mais laisse de grands degrés de liberté dans la manière de faire.

L'implémentation concrète n'est pas précisée, ce qui est propre à toute norme 'système de gestion'.

On notera dans le contexte français -qui privilégie l'approche par les risques et les moyens- que le BIA (approche par les processus) est obligatoire. Il y aura en France du travail à faire !

Cette norme en devenir représente somme toute un compromis intelligent et pragmatique entre les directives vagues et les détails inapplicables. Mais, le rôle des RPCA, chefs de projets et consultants pour la mise en oeuvre sera très important.

Emmanuel Besluau
Vendredi 28 Janvier 2011

Source :
http://www.duquesnegroup.com

REFACTURATION EN INTERNE DES PRESTATIONS INFORMATIQUES : MODE D'EMPLOI

Par Frédéric Bordage (2007)

En refacturant ses prestations auprès des directions métier, la DSI apporte plus de visibilité aux décideurs fonctionnels. D'un centre de coût, elle devient un des moteurs de croissance de l'entreprise. Les conseils d'un spécialiste.

Nombre de directions des systèmes d'information (DSI) s'interrogent sur l'opportunité de refacturer leurs prestations en interne afin de faire tomber l'image de "boîte noire" de l'informatique et justifier des dépenses engagées en fonction des objectifs métiers ou stratégiques. Ce processus conduit à clarifier le budget, les dépenses et les moyens de répondre aux demandes d'évolution du système informatique. Spécialiste du domaine, wpo@enoraconsulting.com William Porret, directeur associé d'Enora Consulting, a bien voulu répondre à nos questions pour faire un point complet sur le sujet.

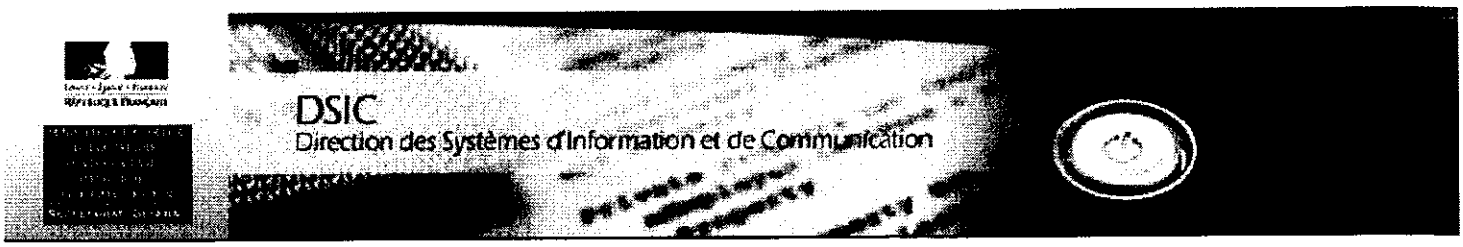
- ***Quels sont les bénéfices de la refacturation des prestations informatiques en interne ?***
  William Porret : Refacturer en interne les prestations informatiques place la DSI au coeur de la gouvernance de l'entreprise. Les moyens informatiques deviennent un élément à part entière du business, de la stratégie et de la croissance. La DSI est alors perçue comme une direction qui apporte des solutions concrètes au business et qui sait chiffrer ses apports. La DSI n'est plus la boîte noire de l'entreprise où les investissements ne sont pas directement liés à la production. Au contraire, tous les investissements et les coûts de fonctionnement sont directement rattachés aux métiers de l'entreprise et valorisés.

- ***Quels sont les principaux freins à la mise en place cette pratique ?***
  Il y en a essentiellement deux. Auparavant, les coûts liés à l'informatique étaient inscrits uniquement dans les budgets consolidés de l'entreprise. Quand les directions métier voient soudain apparaître les coûts informatiques dans leur budget, elles bloquent. Pour surmonter ce handicap, on peut commencer par refacturer la direction générale de l'entreprise plutôt que les différentes directions. Le second frein est lié à la DSI elle-même qui a souvent du mal à évaluer correctement l'ensemble de ses coûts et de ses budgets. Pour contourner ce deuxième obstacle, il faut mettre en oeuvre la gestion des niveaux de service car elle permet d'identifier tous les services délivrés par la DSI et de les suivre finement.

- ***Existe-t-il un modèle idéal de refacturation ?***
  Non. Les entreprises optent soit pour un mode forfaitaire, soit pour une redistribution des coûts constatés. Dans le premier cas, le montant du forfait est fixé en début d'année et revu en fin d'année pour s'adapter aux coûts réels engagés. Ce système a l'avantage de rassurer les directions métiers en apportant une visibilité sur le budget à engager. La redistribution des coûts constatés consiste à refacturer chaque mois ou en fin d'année chaque direction de l'entreprise en fonction des prestations consommées. Plus transparent pour tous et plus proche de la réalité, ce fonctionnement demande du temps et une gestion administrative conséquente afin de calculer précisément les différents coûts afférents à chaque direction.

- ***Comment les DSI chiffrent-elles leurs prestations ?***
  Elles se basent sur leur budget annuel, distinguent les coûts directement imputables à chaque direction et répartissent les coûts indirects. Il faut faire attention à bien tenir compte des coûts propres à la DSI : formation des personnels, coûts de fonctionnement, etc.

- ***Quelle est l'influence d'ITIL sur la refacturation interne ?***
  La méthode ITIL propose des processus de gestion financière de la DSI. Elle classe les DSI en trois catégories selon leur degré de maturité financière. En niveau 1, le plus faible, la DSI est un centre comptable et ne procède à aucune refacturation. En niveau 2, elle est un centre de recouvrement et refacture ses coûts en fonction des utilisateurs et de leurs demandes de services. En niveau 3, elle est un véritable centre de profit. Elle présente alors une organisation financière autonome qui assimile harmonieusement les notions de budget, de coût et de besoins utilisateurs.



Hébergement d'application

A qui s'adresse cette offre ?

La présente offre de service décrit l'ensemble des prestations fournies par le Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration (MIOMCTI), dans le cadre de l'hébergement d'une application.

Cette offre de service s'adresse aux entités du MIOMCTI, ainsi qu'aux organismes qui, quel que soit leur ministère de tutelle, souhaitent faire héberger une application.

Chiffres-clés

Trois centres informatiques nationaux supervisés en 24/7 et sécurisés

Une équipe de 400 agents répartis sur l'ensemble des sites

450 applications du MIOMCTI et d'autres ministères hébergées

2300 serveurs physiques et virtualisés

2000 m² de plateaux d'hébergement

Chaque site possède son secours

Les avantages

L'hébergement d'une application dans l'un des centres d'exploitation du MIOMCTI garantit un niveau de sécurité et de disponibilité élevé grâce à :

- **Des équipes d'exploitation expérimentées et compétentes**
- **Un suivi régulier de la qualité de service**
- **La variété des accès réseau disponibles**

La sécurité

- **Une gestion fine des privilèges et droits administrateurs**
- **La sécurité et la maîtrise des réseaux de transport des informations**
- **Le filtrage des flux applicatifs**
- **La détection d'intrusion**
- **La confidentialité des informations hébergées**
- **Les mécanismes de PRA mis en œuvre dans ces centres**

Notre Offre en quelques mots

L'offre de service « hébergement d'application » vise à proposer l'accueil et l'exploitation des applications métiers et bureautiques des ministères.

Cette offre contient des prestations standards et complémentaires distinguées par niveau de service.

Nos centres d'hébergement peuvent accueillir vos applications sur des infrastructures dédiées ou mutualisées en environnement physique ou virtualisé. Nos sites disposent de technologies de très haute disponibilité avec des accès physiques sécurisés.

Les plates-formes du MIOMCTI sont raccordées à différents réseaux de communication, permettant aux agents des ministères et des partenaires d'accéder aux applications hébergées :

- RGT et Saphir NG (WAN assurant les échanges d'informations entre les différents sites métropolitains et ultra-marins du MIOMCTI)
- ADER (Administration en réseau)
- INTERNET

Le périmètre des prestations incluses dans l'offre est le suivant : exploitation, supervision et administration technique des applications.

En complément, il est possible de souscrire aux prestations :
- Exploitation et supervision applicative
- Gestion des environnements hors production
- Support utilisateur niveau 1
- SAS d'échange applicatif
- Sécurisation/confidentialité avancées

Cette offre de service ne comprend pas les prestations suivantes :
- Hébergement de sites Intranet / Internet (offre dédiée)
- Raccordement au réseau RGT
- Prise d'appel utilisateur et support fonctionnel
- Gestion du poste de travail utilisateur (offre dédiée)
- Supervision des LAN des sites des utilisateurs (offre dédiée)

Le coût défini pour le service d'hébergement n'est valable qu'en cas de respect du cadre de cohérence technique du MIOMCTI (CCT). Toute dérogation au CCT fera l'objet d'un coût spécifique.

Les prestations et logiciels de notre offre

Prestations :

- **Exploitation technique des applications** : sauvegarde, stockage, archivage, ordonnancement, journalisation, traitements courants
- **Supervision technique** : monitoring des serveurs, du LAN Datacenter, des baies et des bases de données, remontée des alertes techniques aux équipes d'exploitation
- **Administration technique:** installation et configuration des serveurs et réseaux
- **Gestion de la sécurité logique** : maintien en condition de sécurité
- **Gestion des incidents de production** (hors incident fonctionnel), **des changements, problèmes, mises en production**
- **Gestion de la capacité, de la disponibilité, de la continuité (PCA, PRA)**
- **Gestion de la sécurité physique** : accès aux centres d'hébergement, détection incendie, ...
- **Gestion des fluides** : électricité, climatisation

Les logiciels inclus dans notre offre sont conformes avec le CCT du MIOMCTI.

Exemple de logiciels du pack standard :

- Systèmes d'exploitation : Centos, Debian GNU/Linux, Windows Server, Unix AIX
- Tiers de presentation : Apache / Tomcat
- Bases de données : Oracle, PostgreSQL, MySQL
- Outils de supervision : Nagios

Les différents niveaux de service proposés

	Platine	Or	Argent	Bronze
Architecture	Très haute disponibilité	Haute disponibilité	Mécanismes de reprise d'activité	Mécanismes de reprise d'activité
Perte de donnée maximale	Aucune perte (hors transaction en cours)	2h	24h	48h
Disponibilité sur la plage d'ouverture du service (hors WAN et arrêts planifiés)	L'application est accessible en permanence, y compris en cas d'incident sur la plateforme d'exploitation 99,9% (< 8h par an)	L'application est disponible sauf le temps de bascule automatique en cas de : • sinistre • incident bloquant 99,5% (<2j par an)	L'application est disponible sauf : • temps de bascule manuelle en cas de sinistre • créneaux de maintenance • temps de résolution en cas d'incident bloquant 98% (<8j par an)	L'application est disponible sauf • le temps de sa reconstruction en cas de sinistre • créneaux de maintenance • temps de résolution en cas d'incident bloquant 95% (<20j par an)
Durée max d'une indisponibilité (hors arrêts planifiés)	1h	4h	24h	96h
Nb max d'indisponibilité / an (hors arrêts planifiés)	12	12	16	16
Délai de résolution d'un incident bloquant	80% des incidents sont résolus en moins de 30mn	80% des incidents sont résolus en moins de 2h	80% des incidents sont résolus en moins de 16h	80% des incidents sont résolus en moins de 48h
Ouverture du support technique (horaire de métropole)	Tous les jours 24h/24h	Tous les jours 24h/24h	Du lundi au vendredi de 8h à 18h	Du lundi au vendredi De 8h à 18h

Prestations complémentaires possibles

- Exploitation applicative : gestion des échanges applicatifs et requêtes à façon
- Supervision applicative : alertes applicatives
- Gestion d'environnement hors production : développement, formation, intégration, qualification, pré-production
- Support utilisateur niveau 1
- SAS d'échange pour les flux entre applications
- Sécurisation et confidentialité avancées des flux